IAB Minutes
November 8, 2005

The Interagency Advisory Board (IAB) Meeting convened on Tuesday, November 8, 2005 at 9:00 AM in the American Institute of Architects (AIA) Auditorium. The meeting was chaired by Mike Butler. After his introductory remarks, the following agenda items were presented and discussed.

A. **HSPD-12 Enterprise Training Initiative – Bob Donelson (DOI).** The various HSPD-12 training tools that have and are being developed were discussed. Key points:

- Module 1: *Homeland Security Overview* is available on CD now (contact brant.petrick@gsa.gov) and will be available at www.usalearning.gov within a few weeks.
- Module 2: *PIV Roles and Responsibilities* is available on CD (contact brant.petrick@gsa.gov) and online at www.vodium.com/goto/blm/hspd12.asp
- Module 3: *Privacy*, Module 4: *PIV Credential Technology*, and Module 5: *PIV Credential Uses*, are under development and are expected in April 2006.
- There were 508 compliance issues with the first version of Module 2, both for CD and online versions. This has been resolved in the latest release of Module 2.

B. **Physical Access Interagency Interoperability Working Group (PAIIWG) – Mike Sulak (Dept. of State).** Key Points:

- PACS 2.2 has been updated to version 2.3E. This is an update, not a rewrite
- There was discussion regarding the “NACI complete” indicator, and the decision to NOT include that data item in the CHUID. Achieved consensus that the NACI indicator is not related to physical access and should not be part of the CHUID
- The PAIIWG is looking for quick approval of PACS 2.3E by the IAB
- A vote will be taken electronically
- The PAIIWG plans to begin work on PACS v3.0 in the beginning of 2006.

C. **Smart Card Alliance Physical Access Council – Dwayne Pfeiffer (SCA).** Key Points:

- This Council is one of several new SCA technology and industry councils
- Goal is to foster increased collaboration within PACS industry and produce tangible results
- Have developed a whitepaper on FIPS 201 and Physical Access Control
- Available at: http://www.smartcardalliance.org/alliance_activities/FIPS_201_Impact.cfm
- Have developed a FIPS 201 Compliance Presentation targeted to Government
    - Provides a clear understanding of what FIPS 201 compliance means for PACS
    - Will begin presenting mid to late November
    - Covers cards, readers, hosts & panels, infrastructure, biometrics, privileges, C&A

D. **Interagency Partnership Working Group (IPWG) – Lolie Kull (DHS).** Key Points:

- The Goals of the IPWG are (a) reduce overall cost to the government, (b) combine efforts and resources for implementation and (c) ensure interoperability and operational success
- Focused on 4 key functional areas: Enrollment, Card Issuance, Card Management, and Identity Management System (IDMS)

- Current participants include: DHHS, DHS, DOC, DOI, DOJ, DOL, DOT, Education, EAP, GPO, GSA, HUD, USDA, IBB, OPM, SBA, SSA, DOS, Treasury, USPS, VA, NARA
- Other agencies are welcome to join
- Charter approved October 19, 2005
- The Postal Service (USPS) is piloting a program for offering PIV identity proofing services at selected post offices
- The Office of Personnel Management (OPM) plans to use these services at 10 locations across the US
- GSA is creating an Interagency Agreement (IA) to allow agencies to enter the pilot, and a Financial Addendum (FA) to allow payments through GSA
- Questions: Lolie.kull@dhs.gov or Eric_M._Stout@hud.gov

E. **HSPD-12 and Privacy – Eric Stout (HUD).** A summary of privacy requirements related to HSPD-12 was presented. Key Points:

- OMB M-05-24 levies 7 privacy requirements. Of these, 3 were elaborated on
- #3 Privacy Impact Assessment (PIA), required for systems/databases supporting PIV processes. The Interagency Privacy Committee is working on sample PIAs to offer agencies
- #4 Federal Register Notice, required for 30 day public comments and explains "routine uses" and disclosures allowed. The Interagency Privacy Committee is working on model language
- #6 Privacy polices, should include Privacy Act statement, complaint/appeals procedures, and sanctions for violations
- Questions should be referred to agency Privacy Act Officer, Eva_Kleederman@omb.eop.gov or Jeanette_I._Thornton@omb.eop.gov

F. **Joint Program Handheld/Mobile Device Status – Frank Jones (DoD).** Key Points:

- There are many different handheld devices available, and multiple applications
- Still trying to identify a core set of widely applicable requirements, and soliciting support for capturing those requirements. Vendor selected to conduct survey.
- Current plan of action shows next two steps are requirements validation by user community and release of RFI to vendor community
- Considering requirements for: general/size/weight, processor/memory, case hardening, display/screen, keypad/buttons, communications/networking, power/battery, data entry capabilities, operating system/software, environmental, approvals/certifications, warranty, vendor requirements, future/optional
- User community consisting of 7 organizations already surveyed
- Seeking IAB support for additional federal participants in requirements survey as well as expertise in expected operating environment

G. **GSA Conformance Testing – April Giles (GSA).** Key Points:

- GSA's FIPS 201 Test Program will determine the products and services that comply with FIPS 201 performance, interoperability, and security requirements; this will result in an Approved Product/Service List (APL) for acquisitions

- Test procedures are expected by February 2006
- Currently have 42 pages of requirements and 53 categories of items
- Products/services cannot be purchased from the BPA until on the approved list
- Looking for volunteers to participate in the FIPS 201 Products/Services Test Program Working Group
- Work Items for the work group include: requirement traceability matrix, PIV product/service categories, test plan, component test /test case/test procedure, test fixtures
- To volunteer, contact April.giles@gsa.gov

H. **Unique Commands – Tim Baldridge (NASA).** A discussion of 4 technical concerns that need to be addressed as work items was presented

- Differences between READ BINARY and GET DATA. SP 800-73 *End-state* cards use GET DATA and not READ BINARY, current implementation (and vendor investments) support PACS 2.2 and 2.3 READ BINARY implementations. Need to resolve this gap
- CHUID Buffer Length TLV omitted from SP 800-73. This appears to be an editorial omission that is easily fixed
- Expiration date coherency. The Card expiration date appears in 3 places: printed on the card, in the CHUID, and in the Printed Information Buffer. There is no clear requirement defining the relationship of these three. It is assumed PKI certificates will expire before the earliest of any of these three
- PIN Protecting the Identity Certificate will break Windows SC logon as implemented in current retail Windows XP versions. Request NIST review this PIN protection requirements for this certificate

I. **DOD DMDC Smart Card Test Harness Suite – Jon Macklin (CUBIC).** Key Points:

- Existing tool for analyzing RIS 3.0 and SmarTrip cards
- Plan to add GSC-IS 2.1/SP 800-73 Transition Card interface
- Supports multiple cards: Philips DesFire (Type-A), Mifare Classic, Mifare UltraLight (Type-A), and Smart MX; and ST19 uP card (Type-B)
- Provides detailed card analysis: card structure, file and memory layout, performance analysis, and encryption/decryption
- Currently works with File System cards which is the same operating system supported by Cubic's electronic purse cards. The test harness will be compatible with VM cards
- Goals: Test a minimum of 3 dual-interface reader and card types, and verify the conformance of each to the SP800-73 specification (performance & functionality)

J. IAB Authentication Schema, Desktop to the Back-Stop - Greta Lehman (DoD). Key Points:

- Recommend against placing a *NACI Complete* indicator on the card (in the chips)
- Recommend allowing backend systems to satisfy FIPS 201 "electronically verifiable" requirement, eliminating need for card updates for NACI complete
- OMB has tasked the IAB to "propose an architecture for authentication and vetting status with web services to replace NACI indicator"

- Alternatives must include: systems and token interoperability, credential cross recognition, open architecture design, leveraging existing infrastructure investments, scalability, and ability to include options beyond basic functionality
- Propose a working group to explore options - looking for volunteers

K. **IAB Path Forward - Mike Butler (DoD) and Tony Cieri (DOI)**.

- Presentation posted at www.smart.gov/iab
- Policy and Standards phases complete. IAB to focus totally on implementation phase.
- Connections with industry alliances critical to success.
- Reform IAB to develop much stronger joint partnerships with industry alliances, both technical and application. SCA, IBIA, SIA, APTA used as examples.
- Discussion followed. This proposal was approved by attendees.
- Work to commence starting with SCA.

L. Closing - Mike Butler (DoD)

- IAB Voting members to vote on PAIIWG PACS 2.3E revision via email
- Requested support for established working groups as follows:
  - DoD Testing Group
  - GSA Conformance Testing – April Giles
  - Governance Meeting – rules on how we do business
  - Data Model & Architecture Working Groups – Jim Zok and Tim Baldridge
  - Web-based Authentication – Greta Lehman
  - Sponsorship – Chaired by SEC, FICC and small agency council
  - Partnership – Bob Donelson and Lolie Kull asked to merge efforts to one focus.

The IAB Meeting was adjourned at 12:30 PM.